La NSA según los Documentos Filtrados por Snowden

rafael@bonifaz.ec

Las revelaciones de Snowden

E.Snowden

G. Greenwald

L. Poitras

theguardian

The Washington Post

The New York Times

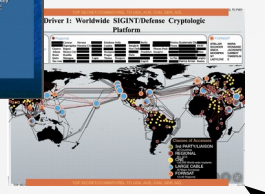
The Intercept_

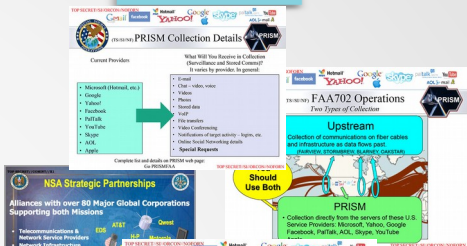
L'espresso

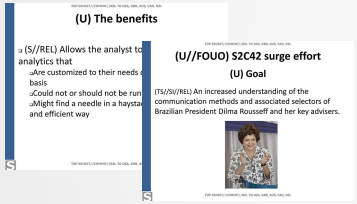
DER SPIEGEL

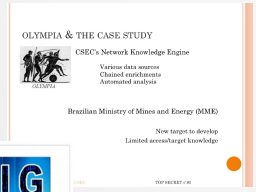
O GLOBO

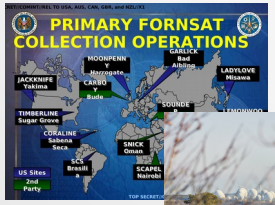
Varias historias

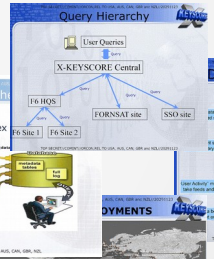


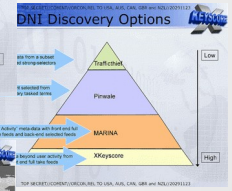


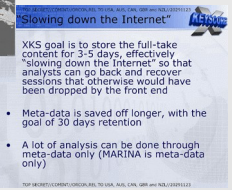


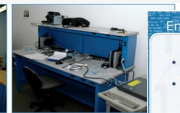


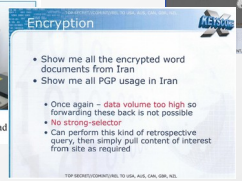


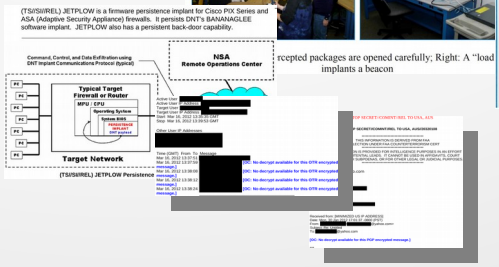












Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

High Speed Optical Cable
Covert, Clandestine or Coorperative Large Accesses

20 Access Programs Worldwide

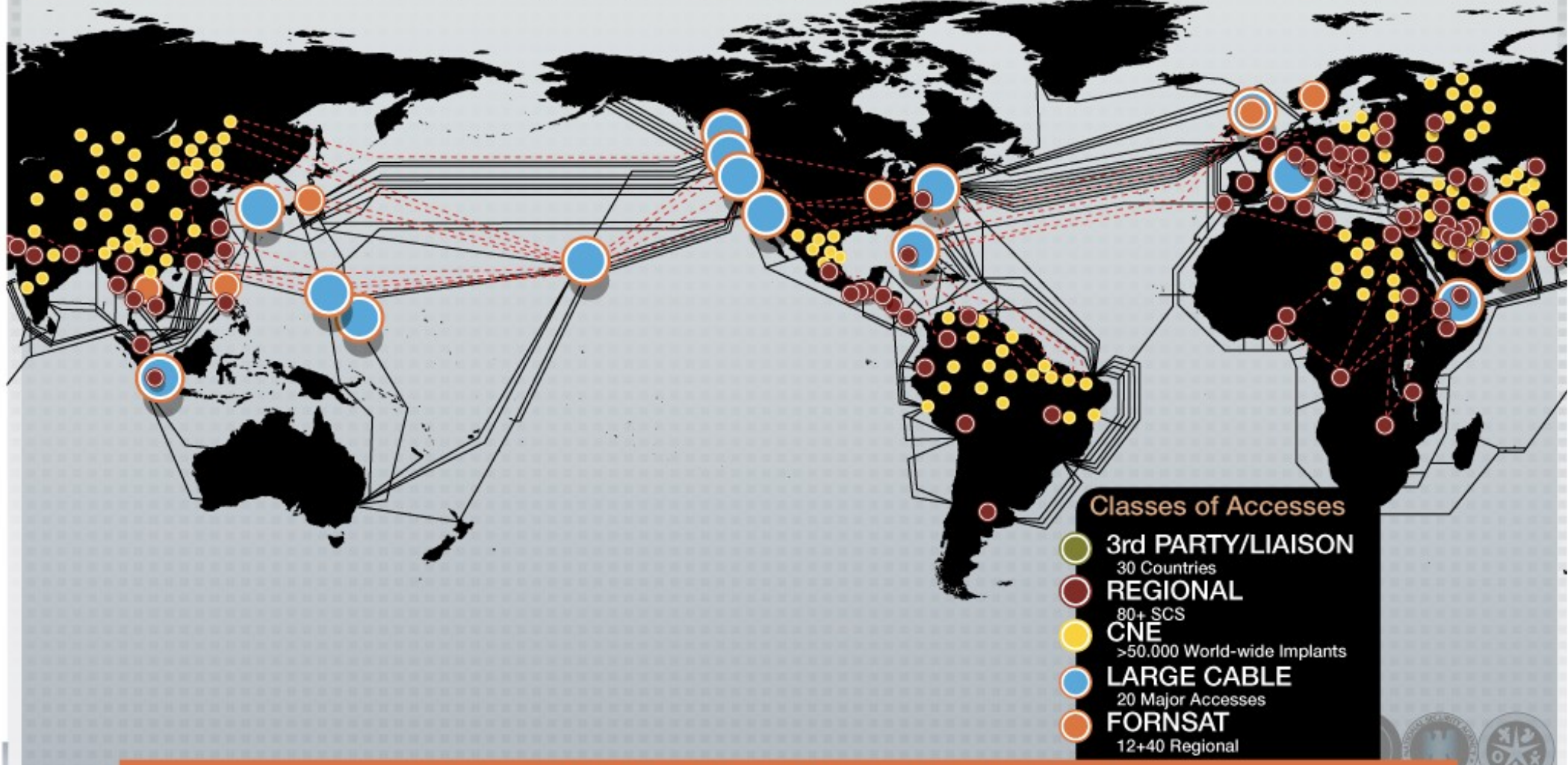
Regional

[redacted]	Caracas	Havana	[redacted]	Kinshasa	Sofia	[redacted]	Berlin	[redacted]	Pristina
[redacted]	Tegucigalpa	Panama City	[redacted]	Lusaka	[redacted]	Bangkok	[redacted]	[redacted]	Tirana
Geneva	Bogota	[redacted]	[redacted]	[redacted]	[redacted]	New Delhi	[redacted]	Phnom Penh	[redacted]
Athens	Mexico City	[redacted]	[redacted]	Budapest	[redacted]	[redacted]	Frankfurt	Sarajevo	[redacted]
Rome	Brasilia	[redacted]	[redacted]	Prague	[redacted]	Paris	[redacted]	[redacted]	[redacted]
Quito	Managua	[redacted]	Lagos	Vienna	Rangoon	[redacted]		[redacted]	La Paz
San Jose	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Zagreb	[redacted]	[redacted]

Guatemala City	[redacted]		
[redacted]	RESC		
[redacted]	[redacted]		
[redacted]	Milan		
[redacted]	[redacted]		
[redacted]	Langley		
Vienna Annex	Reston		

FORNSAT

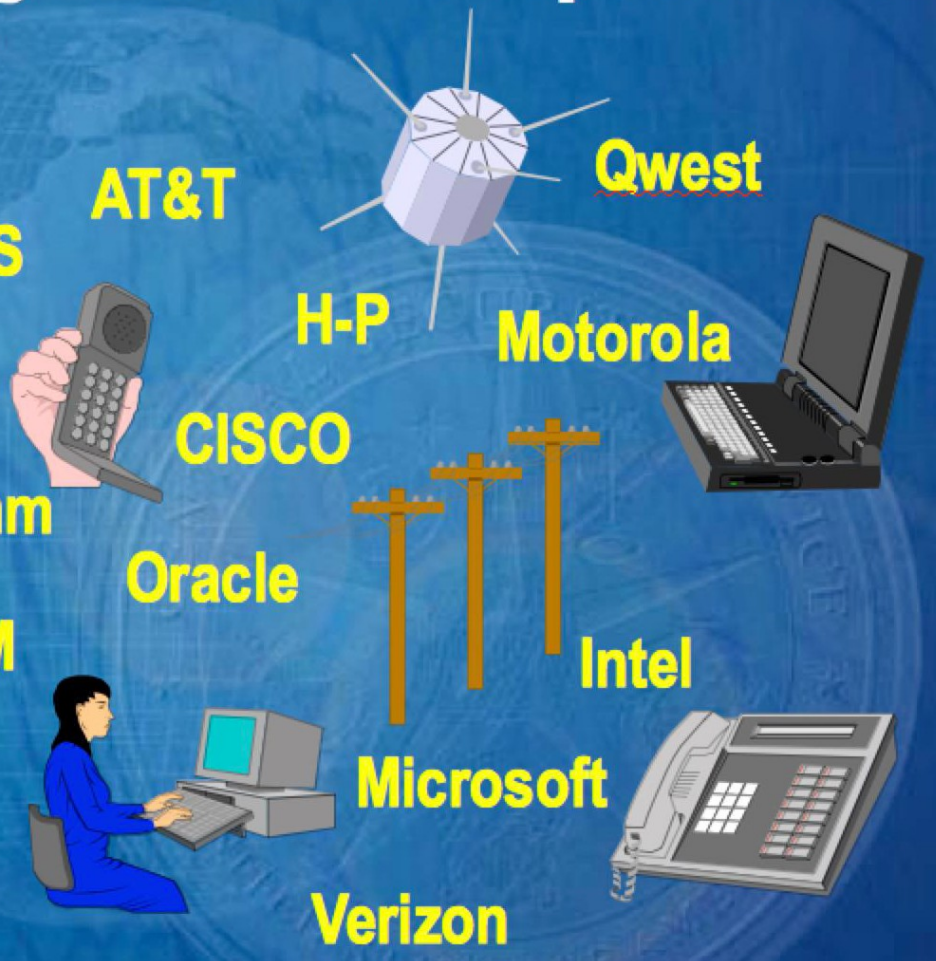
STELLAR	INDRA
SOUNDER	IRONSAND
SNICK	JACKKNIFE
MOONPEN	CARBOY
NY	TIMBERLIN
LADYLOVE	E



NSA Strategic Partnerships

Alliances with over 80 Major Global Corporations Supporting both Missions

- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators



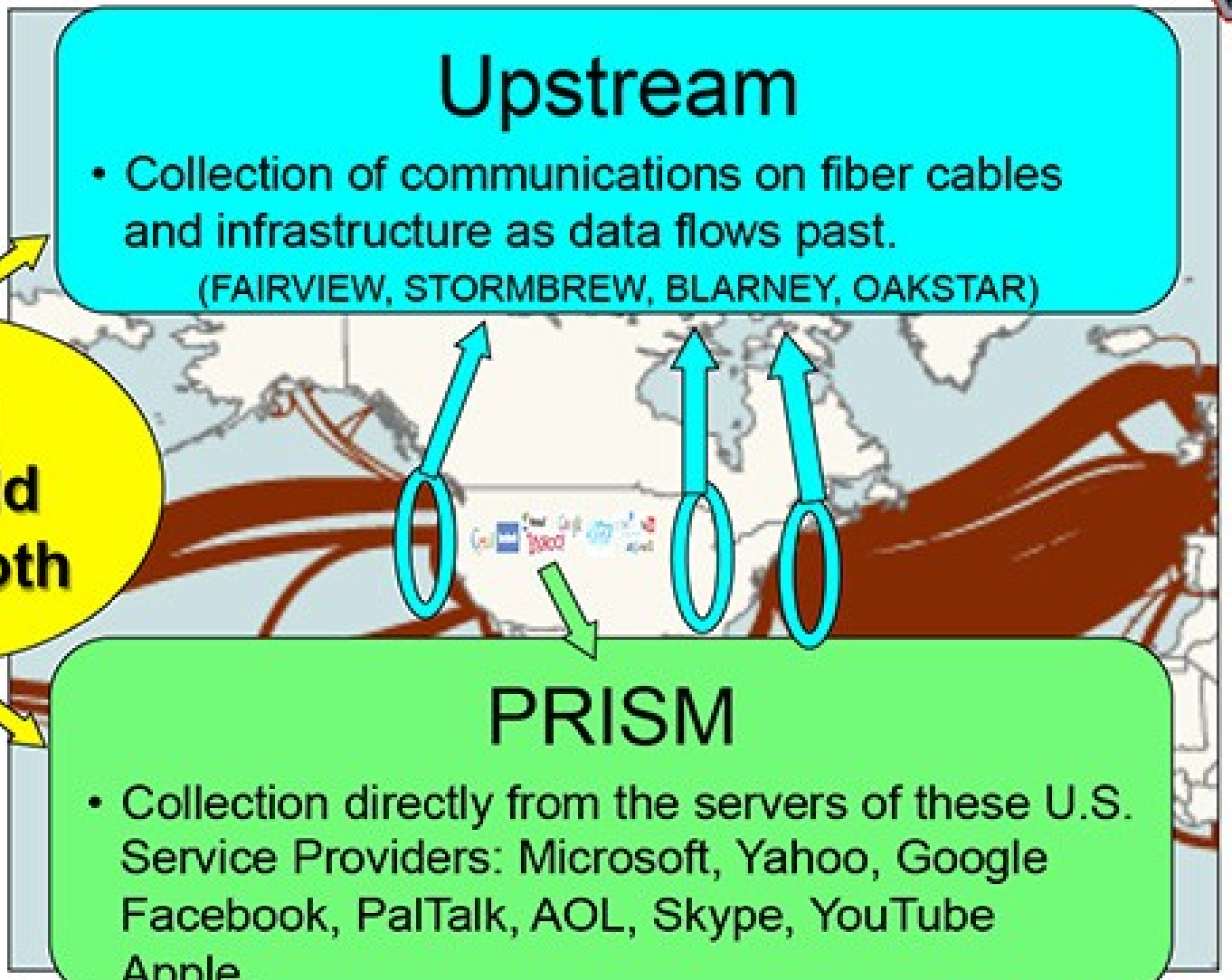
(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)



You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

(TS//SI//NF) PRISM Collection Details

Current Providers

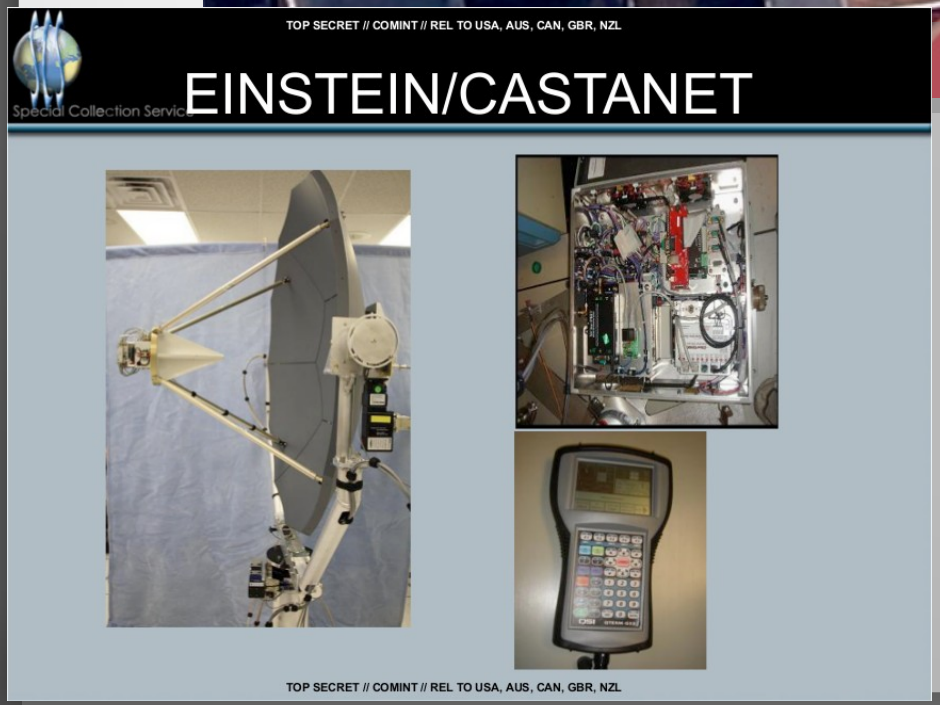
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

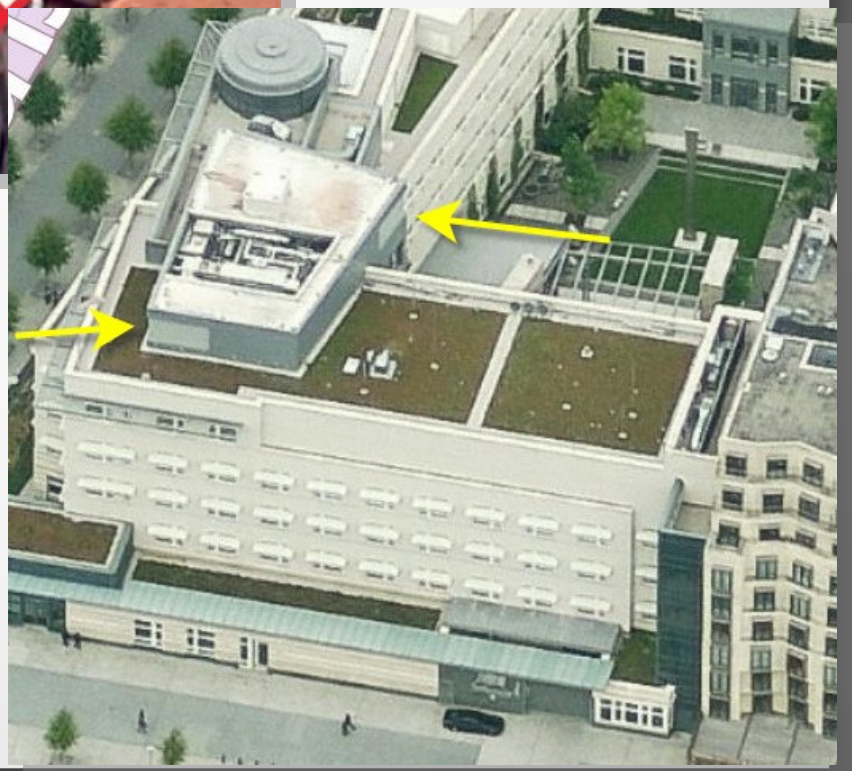
What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

Espionaje en Embajadas

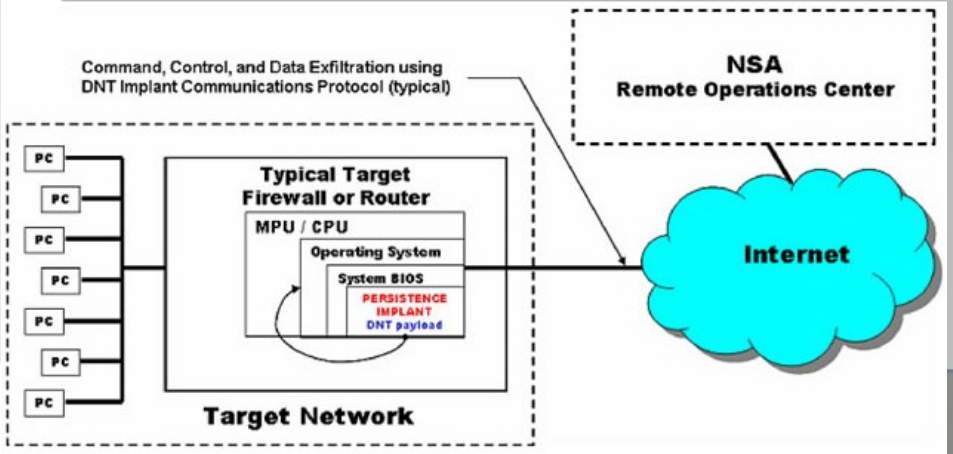




Espionaje a satélites

Ataques Informáticos

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.



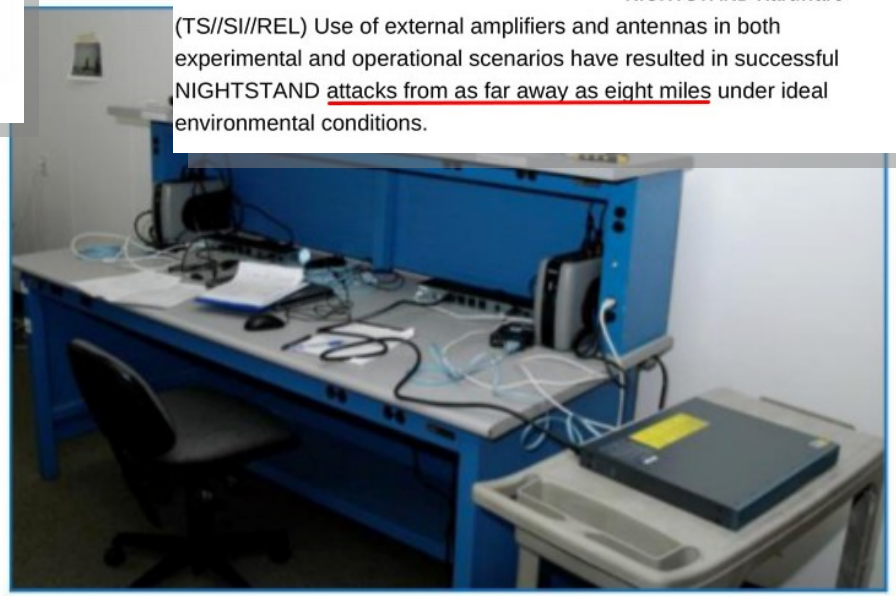
(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

System Details

- (U//FOUO) Standalone tool currently running on an x86 laptop loaded with Linux Fedora Core 3.
- (TS//SI//REL) Exploitable Targets include Win2k, WinXP, WinXPSP1, WINXPSP2 running internet Explorer versions 5.0-6.0.
- (TS//SI//REL) NS packet injection can target one client or multiple targets on a wireless network.
- (TS//SI//REL) Attack is undetectable by the user.

NIGHTSTAND Hardware

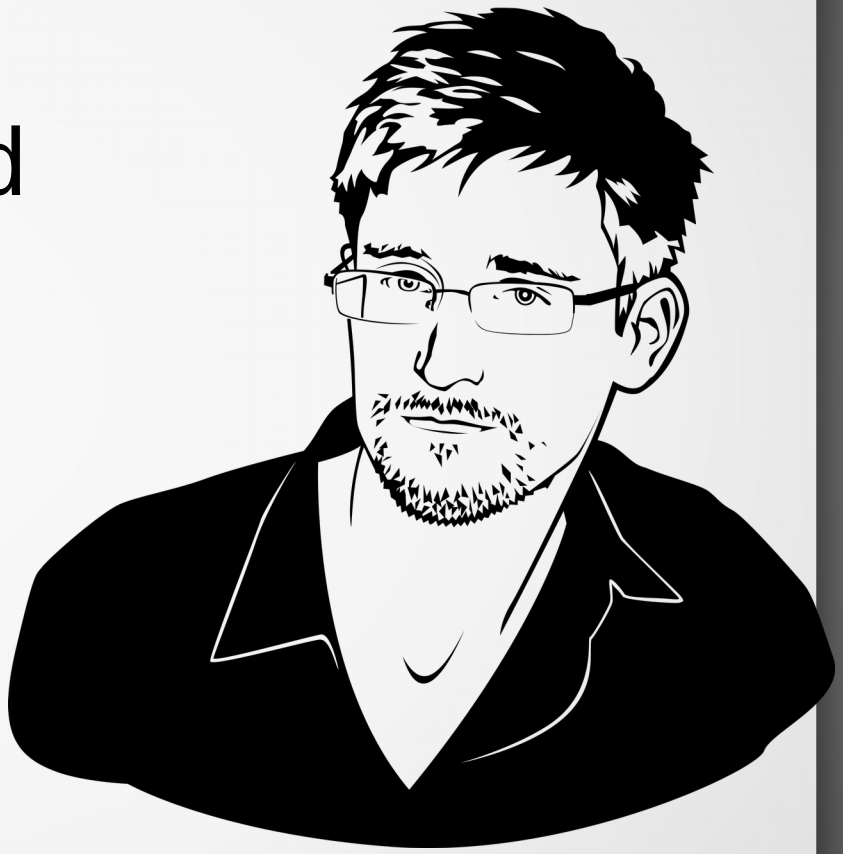
(TS//SI//REL) Use of external amplifiers and antennas in both experimental and operational scenarios have resulted in successful NIGHTSTAND attacks from as far away as eight miles under ideal environmental conditions.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

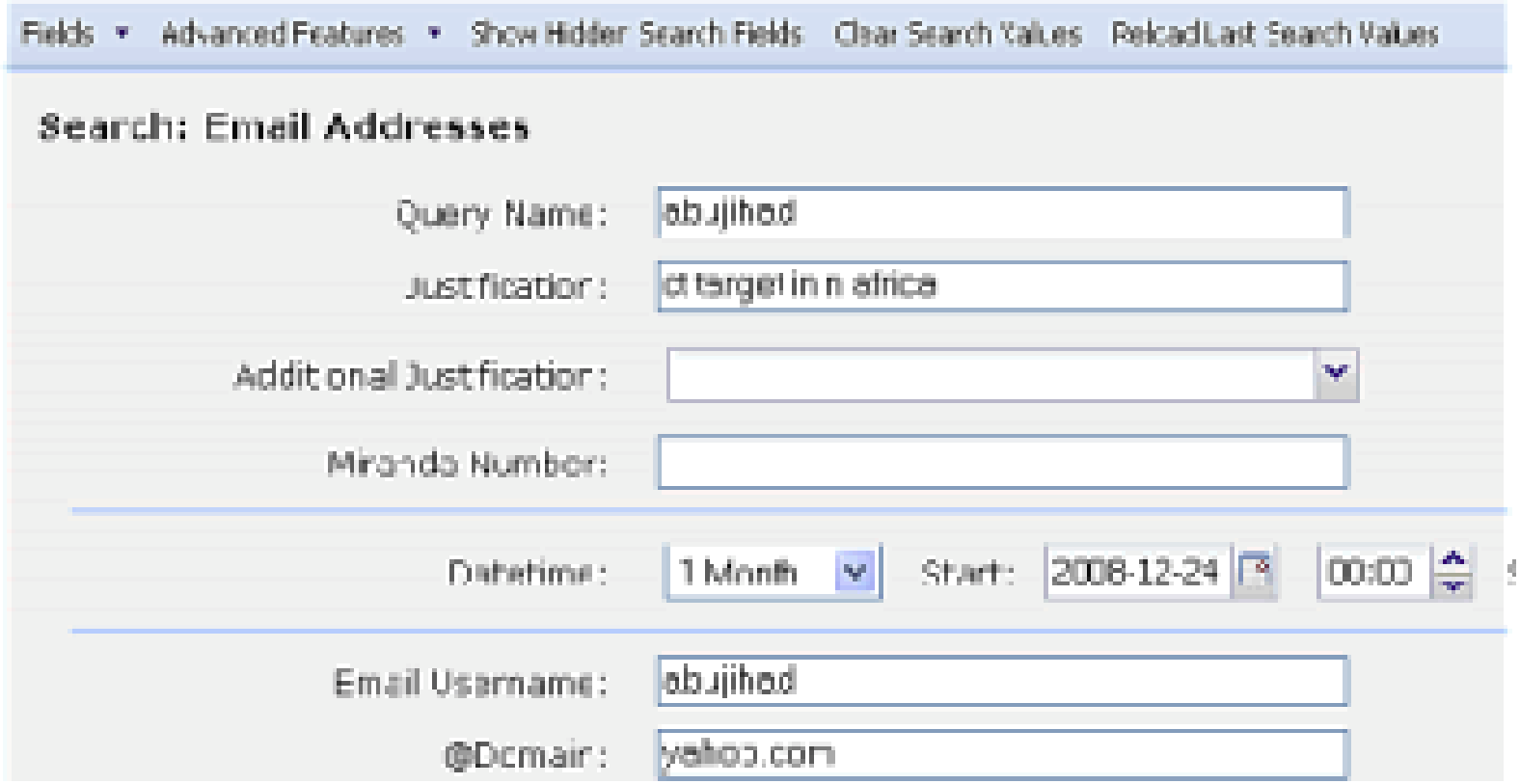
Los Documentos de Snowden

"Yo, sentado en mi escritorio, tenía la facultad de intervenir al que fuera, desde un contador hasta un juez federal e incluso el presidente, siempre y cuando tuviera su correo electrónico personal"

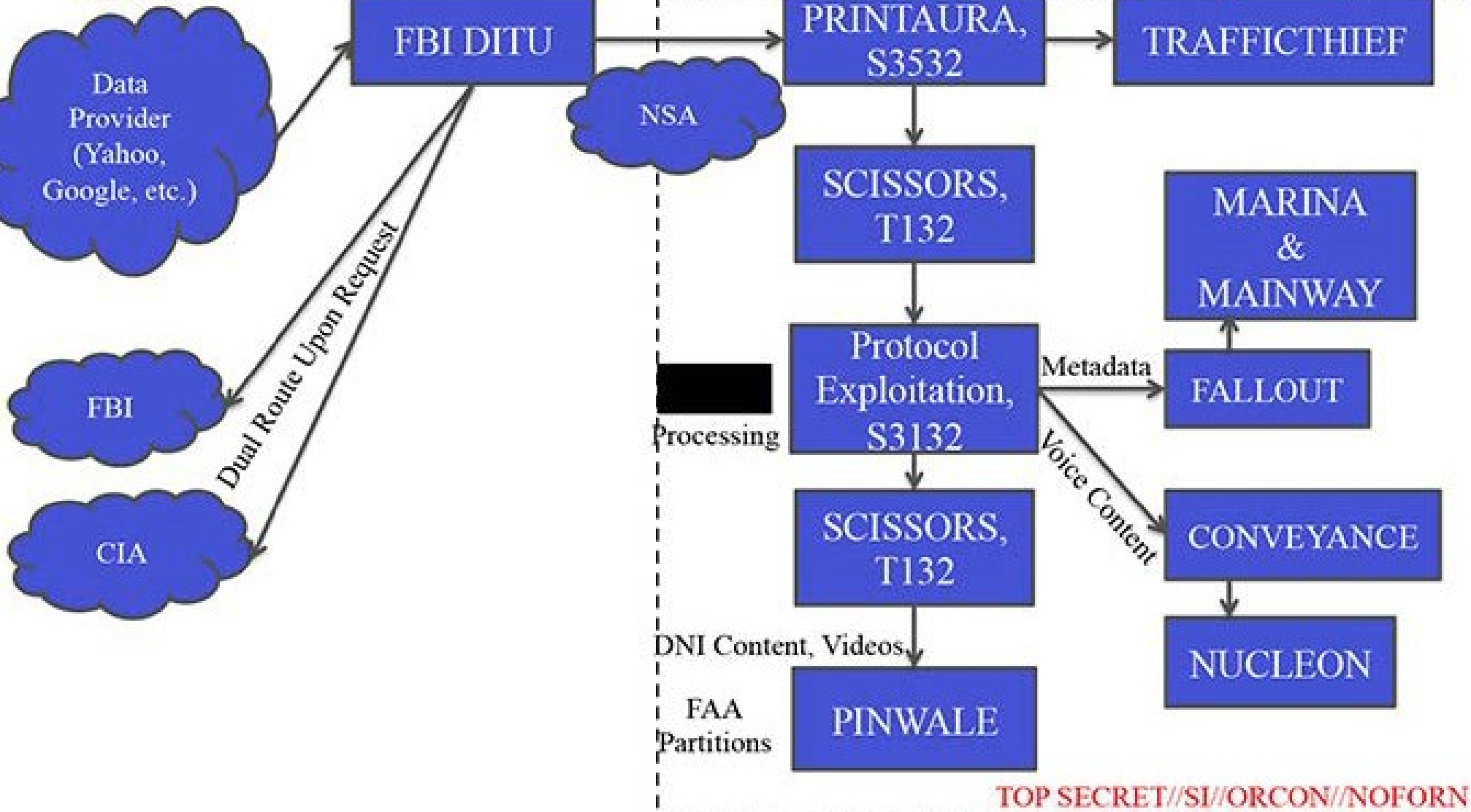


Ej: Buscar correos electrónicos

That would look something like this…



(TS//SI//NF) PRISM Collection Dataflow



Espionaje Político

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C42 surge effort

(U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

UO) S2C41 surge effort

Mexico Leadership Team (S2C41) conducted a two-
pment surge effort against one of Mexico's leading
ates, Enrique Pena Nieto, and nine of his close
considered by most political pundits to be the likely
Mexican presidential elections which are to be held
leveraged graph analysis in the development
opment effort.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

Espionaje a sysadmins

TOP SECRET STRAP1 **TOP SECRET**

Employees:

Christian Steffen [redacted]@stellar-pcs.com or .de - CEO of Stellar DBS
[redacted]@stellar-pcs.com - Engineer
Stellar-DBS NOC noc@stellar-dbs.com - NOC
[redacted]@stellar-pcs.com
Christoph Sommer [redacted]@stellar-pcs.com
Ali Fares [redacted]@stellar-pcs.com
Richard Grave [redacted]@stellar-pcs.com
[redacted]@stellar-pcs.com
Simona Steffen [redacted]@stellar-pcs.com
[redacted]@stellar-pcs.com
Oliver Skaletz [redacted]@stellar-pcs.com

[redacted]

[redacted]@stellar-pcs.com

Employees:

[redacted]@iabg.de
[redacted]@iabg.de
[redacted]@iabg.de

Fuente: http://www.spiegel.de

Software Libre y Criptografía

Active User [redacted]
Active User IP Address [redacted]
Target User [redacted]
Target User IP Address [redacted]
Start Mar 16, 2012 13:35:35 GMT
Stop Mar 16, 2012 13:39:53 GMT

Other User IP Addresses
[redacted]

Time (GMT)	From	To	Message
Mar 16, 2012 13:37:51	[redacted]		
Mar 16, 2012 13:37:59			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:08			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:12			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:24			[OC: No decrypt available for this OTR encrypted message.]

Tor Stinks... (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

TOP SECRET//COMINT//REL TO USA, AUS

TOP SECRET//COMINT//REL TO USA, AUS//20320108

****
THIS INFORMATION IS DERIVED FROM FAA
COLLECTION UNDER FAA COUNTERTERRORISM CERT
****
THIS INFORMATION IS PROVIDED FOR INTELLIGENCE PURPOSES IN AN EFFORT TO DEVELOP POTENTIAL LEADS. IT CANNOT BE USED IN AFFIDAVITS, COURT PROCEEDINGS OR SUBPOENAS, OR FOR OTHER LEGAL OR JUDICIAL PURPOSES.
****

[redacted]@yahoo.com

***

[redacted]

SIGAD: US-984XN
PDDG: AX
CASE_NOTATION: [redacted]
DTG: 31JA0101Z12

Received from: [MINIMIZED US IP ADDRESS]
Date: Mon, 30 Jan 2012 17:01:37 -0800 (PST)
From: [redacted]-[redacted]@yahoo.com>
Subject: Re: Untitled
To: [redacted]@yahoo.com

[OC: No decrypt available for this PGP encrypted message.]

***

Contacto

- rafael@bonifaz.ec
  38B8 6D44 6338 10DF 3334 204E CDFE 5731 6513 8A9F
- Blog: https://rafael.bonifaz.ec
- Microblog: rbonifaz@masotdon.social @rbonifaz